

## Webin uudesta turvasta sovittiin

21.6.2007 12:51 — Matias Mäki [matias.maki@sanoma.fi](mailto:matias.maki@sanoma.fi)

Ssl-sertifikaattien myöntäjien ja selainvalmistajien yhteistyöelin Certification Authority/Browser Forum ilmoitti ratifioineensa sertifikaattien hakijoiden henkilöllisyyden varmistamiseen keskittyvän ev ssl:n ohjesäännöt. Tällä hetkellä kuitenkin Microsoftin Internet Explorer 7 -selain on ainoa uusia sertifikaatteja suoraan tukeva selain.

Extended Validation ssl -sertifikaatti rakentuu nykyisen ssl-muodon päälle. Ev ssl tarjoaa ylimääräisen suojakerroksen tiukasti määritellyn sertifikaatin hakijan henkilöllisyyteen keskittyvän prosessin avulla.

Uuden järjestelmän saumattomuuden vuoksi prosessiin on määritetty helpot ja tehokkaat sertifikaattien mitätöimismahdollisuudet. CABin mukaan kaikki suurimmat nettiselainten tekijät, KDE, Microsoft, Mozilla ja Opera, sitoutuneet uuteen sertifikaattiin ja joko suunnittelevat tai jo tukevat sitä.

Ainoastaan Apple loistaa poissaolollaan, mutta toisaalta Applen Safari-selain perustuu KDE:n KHTML-moottoriin.

CAB on hionut juuri ratifioitua ohjesäännöstöä lähes kaksi vuotta. Sertifikaattien myöntäjistä ohjesäännöt ratifioi muun muassa Entrust, GlobalSign, GoDaddy, Network Solutions, RSA Security, SecureTrust, Swisscom, TDC, Thawte ja Verisign.

Ohjesäännösten mukaan sertifikaatin myöntäjän tulee varmistaa hakijan laillinen, fyysinen ja toiminnallinen olemassaolo ja varmistaa hakija virallisia tietoja vastaan, hakijan oikeudet käyttää kyseistä nimitunnusta sertifikaatissa sekä hakija käyttää ev-sertifikaattia oikein.

Ev ssl:n on tarkoitus parantaa suojattujen nettipalveluiden tietoturvauskottavuutta käyttäjien silmissä. Tällä hetkellä ensimmäinen uutta sertifikaattia suoraan tukeva selain on Microsoftin Internet Explorer 7. Ev ssl -sertifikaatilla varustetulle sivulle surfatessa selaimen osoitepalkki muuttuu vihreäksi ja sivuston omistajasta ja sertifikaatin myöntäjästä kerrotaan lisätietoja osoitepalkin oikeassa päässä.

---

Mozilla Firefox -selaimen 1.5 ja sitä uudemmat versiot tukevat uusia sertifi kaatteja erillisen laajennuksen avulla. Tällä hetkellä kehityksessä oleva Firefox 3 kaavaillaan tukevan ev-sertifikaatteja. Myös Opera on ilmoittanut tarjoavansa tulevissa selainversioissaan ev-tukea.

<http://www.digitoday.fi/tietoturva/2007/06/21/webin-uudesta-turvasta-sovittiin/200715517/66>